Discovery of OSCORE Groups with the CoRE Resource Directory

draft-tiloca-core-oscore-discovery-07

Marco Tiloca, RISE
Christian Amsüss
Peter van der Stok

IETF 109, CoRE WG, November 17th, 2020
Recap

› A newly deployed device:
  – May not know the OSCORE groups and their Group Manager (GM)
  – May have to wait GMs to be deployed or OSCORE groups to be created

› Use web links for discovery – Typically through the Resource Directory (RD)
  – Discover an OSCORE group and retrieve information to join it
  – Practically, discover the links to join the OSCORE group at its GM
  – CoAP Observe supports early discovery and changes of group information

› Use resource lookup, to retrieve:
  – The name of the OSCORE group
  – A link to the resource at the GM for joining the group

› Full support for both Link-Format and CoRAL RD
Updates from -07

› Addressed review of -06 at [1]

› Closed open points raised at IETF 108

› Retrieval for the link to the ACE AS, if also registered
  ‒ Need for a separate lookup (simpler if/when using CoRAL queries)
  ‒ Shown in later example

› Rewording about Link-Format as not typed (-2 vs. “-2”)
  ‒ Limitation for target attributes indicating algorithms
  ‒ Strings that look like integers are not supported
  ‒ Not an issue with current registered algorithms

[1] https://mailarchive.ietf.org/arch/msg/core/3M-ASJxDvrMrSi26-Jk4tl3cmOs/
Updates from -07

- Alignment with other documents
  - rt="core.osc.gm": Moved to draft-ace-key-groupcomm-oscore
  - if="ace.group": Used from draft-ace-key-groupcomm
  - "OSCORE groups" renamed as "Security groups"

- All examples in Link-Format and CoRAL revised accordingly
Updates from -07

Registration

Request: GM -> RD
Req: POST coap://rd.example.com/rd?ep=gml
Content-Format: 40
PayLoad:
</ace-group/feedca570000>;ct=41;rt="core.osc.gm";if="ace.group";
sec-gp="feedca570000";app-gp="group1";
cs_alg="-8";cs_alg_crv="6";
cs_key_kty="1";cs_key_crv="6";
cs_kenc="1",
</coap://as.example.com/token>;rel="authorization-server";
anchor="coap://[2001:db8::ab]/ace-group/feedca570000"
Response: RD -> GM
Res: 2.01 Created
Location-Path: /rd/4521

Discovery

Request: Joining node -> RD
Req: GET coap://rd.example.com/rd-lookup/res
?rel=authorization-server
&anchor=coap://[2001:db8::ab]/ace-group/feedca570000
Response: RD -> Joining node
Res: 2.05 Content
Payload:
<coap://[2001:db8::ab]/ace-group/feedca570000>;rt="core.osc.gm";
if="ace.group";sec-gp="feedca570000";app-gp="group1";
cs_alg="-8";cs_alg_crv="6";cs_key_kty="1";cs_key_crv="6";
cs_kenc="1";anchor="coap://[2001:db8::ab]"

Example involving the link to the ACE Authorization Server
Updates from -07

› Bridge with *draft-ietf-ace-oscore-gm-admin*
  - Followed a suggestion from [2] and discussed at IETF 108
  - Names of application groups specified when creating the security group at the GM
  - *The GM knows those names*, to use them as value of the ‘app-gp’ attribute with the RD

› Multiple security groups may be retrieved for a same application group
  - Useful when different joining nodes support different algorithms
  - A client can join any security group; a server has to join all security groups
  - More details and guidelines are in *draft-ietf-core-groupcomm-bis*

[2] https://mailarchive.ietf.org/arch/msg/core/BoYGYmEpJMUS8bk4PNHOEaFFcdU/
Summary and next steps

› Addressed review of -06 and open points from IETF 108

› Next steps
  – Add target attributes related to the pairwise mode of Group OSCORE
  – Revise the usage of ‘anchor’, based on upcoming core-resource-directory-27
  – Extend security considerations, based on upcoming core-resource-directory-27

› Plan to run first tests against Christian’s RD

› Need for more reviews
Thank you!

Comments/questions?

https://gitlab.com/crimson84/draft-tiloca-core-oscore-discovery
Backup
Application/CoAP/Security Groups

› Application group
  – Defined in {RD} and reused as is
  – Set of CoAP endpoints sharing a pool of resources
  – Registered and looked up just as per Appendix A of {RD}

› CoAP Group
  – Defined in draft-ietf-core-groupcomm-bis
  – Set of CoAP endpoints listening to the same IP multicast address
  – The IP multicast address is the ‘base’ address of the link to the application group

› (OSCORE) Security Group
  – Set of CoAP endpoints sharing a common security material (e.g. OSCORE Ctx)
  – A GM registers the group-membership resources for accessing its groups
Application vs. Security Groups

Security Group 1
- Application Group 1
  - Resources for given function
  - CoAP group with one multicast address

Security Group 2
- Application Group 2
- Application Group 3

Client of application group
- Different key sets
- Resources for given function
The GM registers itself with the RD
- MUST include all its join resources, with their link attributes
- rt="core.osc.gm", if="ace.group"

Request: GM -> RD

Req: POST coap://rd.example.com/rd?ep=gml
Content-Format: 40
Payload:
</ace-group/feedca570000>;ct=41;rt="core.osc.gm";if="ace.group";
    sec-gp="feedca570000";app-gp="group1";
    cs_alg="-8";cs_alg_crv="6";
    cs_key_kty="1";cs_key_crv="6";
    cs_kenc="1",

<coap://as.example.com/token>;
    rel="authorization-server";
    anchor="coap://[2001:db8::ab]/ace-group/feedca570000"

Response: RD -> GM

Res: 2.01 Created
Location-Path: /rd/4521
The device performs a resource lookup at the RD

- Known information: name of the Application Group, i.e. “group1”
- Need to know: name of the OSCORE Group; Join resource @ GM; Multicast IP address
- ‘app-gp’  Name of the Application Group, acting as tie parameter in the RD

Request: Joining node -> RD

Req: GET coap://rd.example.com/rd-lookup/res
?rt=core.osc.gm&app-gp=group1

Response: RD -> Joining node

Res: 2.05 Content
Payload:
<coap://[2001:db8::ab]/ace-group/feedca570000>;rt="core.osc.gm";
  if="ace.group";sec-gp="feedca570000";app-gp="group1";
  cs_alg="-8";cs_alg_crsv="6";cs_key_kty="1";cs_key_crsv="6";
  cs_kenc="1";anchor="coap://[2001:db8::ab]"
Discovery (2/2)

> The device performs an endpoint lookup at the RD
  - Still need to know the Multicast IP address
  - ‘ep’     // Name of the Application Group, value from ‘app-gp’
  - ‘base’    // Multicast IP address used in the Application Group

Request: Joining node -> RD

Req: GET coap://rd.example.com/rd-lookup/ep
   ?et=core.rd-group&ep=group1

Response: RD -> Joining node

Res: 2.05 Content
Payload:
</rd/501>;ep="group1";et="core.rd-group";
   base="coap://[ff35:30:2001:db8::23]"
Alg/key related parameters

New optional parameters for a registered group-membership resource

- (*)(**) cs_alg : countersignature algorithm, e.g. “EdDSA”
- (*) cs_alg_crv : countersignature curve (if applicable), e.g. “Ed25519”
- (*) cs_key_kty : countersignature key type, e.g. “OKP”
- (*) cs_key_crv : countersignature curve (if applicable), e.g. “Ed25519”
- (*) cs_kenc : encoding of public keys, e.g. “COSE_Key”
- (**) alg : AEAD algorithm
- (**) hkdf : HKDF algorithm

Benefits for a joining node, when discovering the OSCORE group

- (*) No need to ask the GM or to have a trial-and-error when joining the group
- (**) Decide whether to join the group or not, based on the supported algorithms